TC

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/014,362	12/11/2001	Masaki Kyojima	J355-037 US	1127

21706 7590 03/30/2006

NOTARO AND MICHALOS
100 DUTCH HILL ROAD
SUITE 110
ORANGEBURG, NY 10962-2100

EXAMINER	
PHILLIPS, HASSAN A	

ART UNIT	PAPER NUMBER
2151	

DATE MAILED: 03/30/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/014,362	KYOJIMA ET AL.	
	Examiner	Art Unit	
	Hassan Phillips	2151	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,9,11,13,16,17 and 22-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,9,11,13,16,17 and 22-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to communications filed January 17, 2006.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on January 17, 2006 has been entered.

Response to Arguments

3. Applicant's arguments filed January 17, 2006 have been fully considered but they are not persuasive. Applicant argued that no prior art discloses the generation of response to challenge based on a unique operation for the client and access privilege proving data that is created from a private key corresponding to the public key assigned to the each service of the server, which enables different access controls for different services using only one unique operation to the client, and prohibits unauthorized access using an unauthorized copy of data, for example, a user's private key. Examiner respectfully disagrees with Applicant's assertions.

4. In regards to Applicant's arguments, as mentioned in previous actions, Examiner maintains Uskela teaches the client performing a decryption involving a key pair for the client, (col. 5, lines 25-32, col. 4, lines 16-45). This operation is unique to the client because the key pair includes a secret key that uniquely identifies the client, (col. 4, lines 25-30, col. 3, lines 31-56, col. 1, line 65-col. 2, line 16). Thus, in the passages cited in previous actions, Uskela clearly discloses the generation of a response to a challenge based on a unique operation for the client and access privilege proving data that is created from a private key corresponding to the public key assigned to each service of the server, (Uskela, col. 5, lines 6-36).

Applicant submits in the remarks that with Uskela, in order to provide each access control for each service, user must have different private keys corresponding to the different services and also the server must have corresponding public keys to the different private keys owned by the user. The user must keep those private keys securely. Examiner has failed to find such teachings in Uskela and feels Uskela teaches otherwise where Uskela discloses, "a service provider can have several key pairs ***of which one***, for instance, ***is saved in the subscriber identity module*** and information on the pair, whose key is saved in the identity module, is entered in the subscriber data." (Uskela, col. 4, lines 30-34). Furthermore, it is also noted that the features upon which applicant relies in the remarks (i.e., "access privilege proving data is in advance prepared from the private key that is unique to the service of the server...the client can show access privilege to each service using individual privilege proving data...in order to enable individual access control for many services, the client

must only have corresponding privilege proving data units which need not be stored securely") are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

5. Examiner has interpreted the claim language as broadly as possible. It is also the Examiner's position that Applicant has not yet submitted claims drawn to limitations, which define the operation and apparatus of Applicant's disclosed invention in a manner that distinguishes over the prior art. Failure for Applicant to significantly narrow definition/scope of the claims implies the Applicant intends broad interpretation be given to the claims. The Examiner has interpreted the claims with scope parallel to the Applicant in the response and reiterated the need for Applicant to define the claimed invention more clearly and distinctly. Accordingly the references supplied by the examiner in the previous office action covers the claimed limitations. The rejections are thus sustained. Applicant is requested to review the prior art of record for further consideration.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) The invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the

applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1, 13, 16, 17, 22-26, are rejected under 35 U.S.C. 102(e) as being anticipated by Uskela, U.S. Patent 6,721,886.

8. In considering claim 1, Uskela teaches a server that provides service to a client comprising: a public-key storage unit for storing a public key assigned to each service, (col. 5, lines 6-16); a challenge generator for generating a challenge to be sent from the server to the client after the server receives a request for the service from the client, (col. 5, lines 20-32); and an access privilege verifier for verifying, using a corresponding public key, whether a prescribed relationship exists between the challenge and a response to that challenge received from the client, (col. 5, lines 20-34); wherein the response is calculated based on a unique operation for the client and access privilege proving data that is created from a private key corresponding to the public key assigned to the each service of the server, (col. 5, lines 25-36).

9. In considering claim 13, Uskela teaches a server that provides services to clients connected to the server via a network, the server comprising: a script interpreter for interpreting script designed to control the contents of the service, (col. 4, lines 46-55).

10. In considering claim 16, Uskela teaches a method executed in a server for providing service to a client wherein a public key is assigned in advance to a service provided by the server, the method comprising the steps of: generating a challenge when a request for the service is received from the client, (col. 5, lines 20-32); transmitting the challenge to the client, (col. 5, lines 20-32); receiving a response to the challenge from the client, (col. 5, lines 20-32); verifying whether a prescribed relationship exists between the challenge and the response by using the public key assigned to the requested service, (col. 5, lines 32-34); and providing the requested service to the client only when the prescribed relationship exists, (col. 5, lines 25-36); wherein the response is calculated based on a unique operation for the client access privilege proving data that is created from a private key corresponding to the public key assigned to the service of the server, (col. 5, lines 25-36).

11. In considering claim 17, Uskela teaches a method executed in a client for requesting service to a server, the method comprising the steps of: receiving a challenge from the server, (col. 5, lines 20-32); executing a unique operation assigned to the client wherein the unique operation is unique to the client, (col. 5, lines 25-36); generating a response based on the challenge received from the server, the result of the unique operation, and access privilege data that is created from a private key corresponding to the public key assigned to the service of the server (col. 5, lines 20-32); and transmitting the response to the server, (col. 5, lines 20-32).

12. In considering claim 22, Uskela teaches a system comprising: a server that provides service to a client, (col. 4, line 46-col. 5, line 36); a public-key storage unit that stores a public key assigned to the service, (col. 5, lines 6-16); a challenge generator that generates a challenge to be sent from the server to the client after the server receives a request for the service from the client, (col. 5, lines 20-32); an access privilege verifier that verifies whether a prescribed relationship exists between the challenge and a response, the response being corresponding to the challenge and received from the client, and the client that requests the service to the server, (col. 5, lines 20-34); the client further comprising: a unique operation executer that executes unique operations assigned to the client, (col. 3, lines 31-56, col. 5, lines 25-36); a response generator that generates the response to the challenge, the challenge being received from the server, wherein the response is calculated based on the unique operation and access privilege data that is created from a private key corresponding to the public key assigned to the service of the server, and the unique operation is unique to the client, (col. 5, lines 20-36).

13. In considering claim 23, Uskela teaches the server sending the challenge to the client with a condition for using the service, (col. 5, lines 20-36).

14. In considering claim 24, Uskela teaches the unique operation is used under conditions that a common cryptographic hash function is assigned to all clients (col. 5,

lines 25-32, col. 4, lines 16-45) and different data is assigned to each client, (col. 4, lines 25-30, col. 3, lines 31-56, col. 1, line 65-col. 2, line 16).

15. In considering claim 25, Uskela teaches a client that requests service to a server, comprising: a unique operation executer that executes unique operations assigned to the client, (col. 3, lines 31-56, col. 5, lines 25-36); an access privilege providing data storage unit that access privilege proving data, the access privilege proving data being created from a private key corresponding to a public key assigned to the requested service and result of a same unique operation to one executed by the unique operation executer, (col. 5, lines 25-36); a response generator that generates a response to a challenge, the challenge being received from the server, (col. 5, lines 20-36); and wherein the response is calculated based on the result of the unique operation and the access privilege proving data, and the unique operation is unique to the client, (col. 5, lines 20-36).

16. In considering claim 26, Uskela teaches the access privilege providing data storage unit included in a portable device, (col. 5, lines 25-36).

Claim Rejections - 35 USC § 103

17. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

18. Claims 9, 11, are rejected under 35 U.S.C. 103(a) as being unpatentable over Uskela in view of Brown, U.S. Patent 6,487,667.

19. In considering claims 9 and 11, although the teachings of Uskela disclose substantial features of the claimed invention, they fail to explicitly teach the server being a web server.

Nevertheless, web servers were well known in the art at the time of the present invention. In a similar field of endeavor, Brown teaches a challenge-response technique that utilizes keys corresponding to web servers in granting access to the web servers, (col. 3, lines 29-65).

Thus, it would have been obvious to a person of ordinary skill in the art at the time of the present invention to modify the teachings of Uskela to show the server being a web server, and the public key assigned to individual an individual web page, or groups of web pages provided to the client. This would have provided a reliable means for authenticating a client before allowing the client to view individual web pages, or groups of web pages, Uskela, col. 1, line 5 through col. 2, line 16.

Conclusion

20. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Hassan Phillips whose telephone number is (571) 272-3940. The examiner can normally be reached on M-F 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Zarni Maung can be reached on (571) 272-3939. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

HP/
3/27/06

ZARNI MAUNG
SUPERVISORY PATENT EXAMINER